Thermal quantum cryptography: Solutions at the microwave regime

Carlo Ottaviani, Cosmo Lupo, Stefano Pirandola
Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, UK

In order to transform quantum key distribution (QKD) into a mature and appealing approach, able to compete with today's conventional cryptographic technology, several problems need yet to be solved. One of these is the implementation at the microwave regime, therefore exploitable in wireless communications. In this context, the appeal of continuous-variable (CV) systems [1] is that they naturally boost the communication rate.

This work investigates free-space thermal QKD at the microwave regime (see top-left and top-right figure), focusing on two distinct approaches. The first consider the Gaussian two-way protocol [2] with thermal states and homodyne detection, used in reverse reconciliation (RR). In this case we find (see bottom-right figure) a positive key rate at the microwave regime even for high loss, not so far from the recently computed secret-key capacity [3] (red line). The thermal variance is $\bar{V} \simeq 5 \times 10^3$, i.e., GHz range at room temperature.

In the second approach we design a novel one-way thermal protocol, with binary encoding and post-selection, which is inspired by the work of Ref. [4], and goes as follows: The sender, Alice, uses two thermal states ρ_u to encode a classical bit of information $u = 0, 1$ with probability $p(u) = 1/2$. The two thermal states have covariance matrix (CM) [1] $\mathbf{V} = 2(n+1)\mathbf{I}$, where $\mathbf{I}$ =diag$(1, 1)$ and n the average number of thermal photons. Their first moments x_u are different and separated by a *distance* d. The thermal states travel to the receiver (Bob) through a quantum channel with attenuation $\eta \in [0, 1]$ which may come from the ration between the detector's solid angle Ω and 4π (see top-left figure).

We then associate an interval Δx to the arbitrary outcome x and compute Bob's probability of obtaining x conditioned on Alice sending the logical values $u = 0, 1$. This is given by the following expression

$$p(x|u) = \frac{1}{2}\left[\mathrm{erf}\left(\frac{x_u + \Delta}{2\sqrt{2V_b}}\right) - \mathrm{erf}\left(\frac{x_u - \Delta}{2\sqrt{2V_b}}\right)\right], \qquad (1)$$

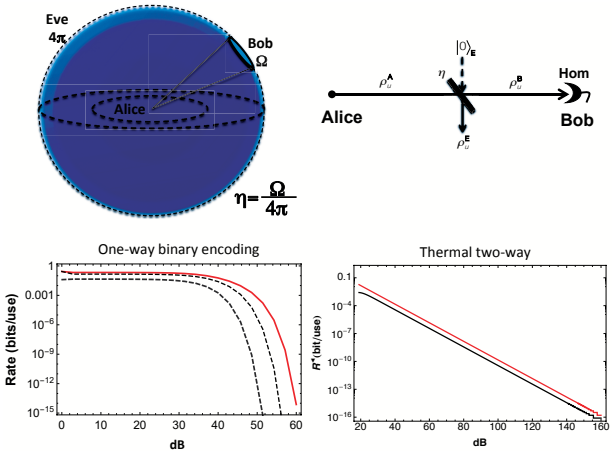
where $x_0 = 2x + \sqrt{\eta}d$, $x_1 = 2x - \sqrt{\eta}d$ and V_b is the variance of the output states received by Bob. From $p(x|u)$, we compute Bob's error probability $p_{err} = [1+\exp(-x\sqrt{\eta}d/V_b)]^{-1}$, and we derive Alice and Bob's mutual information $I_{AB} = 1 - H_2(p_{err})$, where $H_2(p) := -p\log_2 p - (1-p)\log_2(1-p)$. For Eve we compute $I_E = 1 - H_2(p_{eve})$, where $p_{eve} = \frac{1}{2}[1 - \mathrm{erf}(\sqrt{(1-\eta)/(2V_e)}d/2)]$, with V_e being the variance of the states received by Eve. We also bounded Eve's accessible information by using the fidelity and the Pinsker's bound [5].

For all these cases we computed the raw key rate $R_r = I_{AB} - I_{Eve}$ and therefore post-selected key-rate

$$R := \int_\Sigma dx\, p(x,d) R_r(x,d), \qquad (2)$$

which is integrated over the region Σ such that $R_r > 0$, accounting for the density probability, $p(x,d) = p_\Delta(x,d)/\Delta$ associated with outcome x. The key rates for the binary protocol are summarized in the bottom-left figure. The red curve is obtained the fidelity bound, while the gray curve is obtained by computing the Pinsker's bound.

In conclusion we found that the approaches described above allow us to achieve a high key rate in the presence of remarkable amounts of trusted thermal noise and in very attenuated channels. This may pave the way towards free-space communication at the GHz range.



[1] C. Weedbrook *et al.*, Rev. Mod. Phys. **84**, 621 (2012).
[2] C. Weedbrook *et al.*, Phys. Rev. A **89**, 012309 (2014).
[3] S. Pirandola *et al.*, Preprint arXiv:1510.08863 (2015).
[4] Ch. Silberhorn *et al.*, Phys. Rev. Lett. **89**, 167901 (2002).
[5] A. Fedorov, IEEE trans. on Info. Theory **49**, 2003.